What's claimed is:

Claim 1 (Original) A digital signature scheme based on braid group conjugacy problem, parameters involved in this scheme comprising a signatory S, a signature verifying party V, a message M needing signature, an integer n for the number of generators in the braid group, an integer m for the number of generators in the left subgroup, an integer l for the upper bound of the length of a braid, a braid group $B_n(l)$, a left subgroup $LB_m(l)$ of $B_n(l)$, a right subgroup $RB_{n-l-m}(l)$ of $B_n(l)$, a one way hash function h from bit sequence $\{0,1\}^*$to braid groups $B_n(l)$; said signature scheme comprising the following steps of:

Step 1. the signatory(S) selecting three braids $x \in LB_m(l), x' \in B_n(l), a \in B_n(l)$, and making them meet $x'=a^{-1}xa$, moreover, with known x and x', it being impossible to find a in calculation, and considering braid pair(x',x) as a public key of signatory *(S)*, braid a as a private key of signatory *(S)*;

Step 2. signatory (S) using hash function h for message (M) needing signature to get $y=h(M) \in B_n(l)$;

Step 3. generating a braid $b \in RB_{n-l-m}(l)$ at random, then signing the message (M) with the own private key a and the generated random braid b to obtain $Sign(M)=a^{-1}byb^{-1}a$; and

Step 4. the signatory *(S)* outputting message *(M)* and the signature of message (M) *Sign(M)*.

Claim 2 (Original) The digital signature scheme based on braid group conjugacy problem according to claim 1, wherein generating the public key braid pair (x',x) and the private key braid a of signatory (S) in said step 1 comprises the following steps of:

Step 1a. selecting a distance d between system parameter braid groups public key pairs;

Step 1b. representing x into the left canonical form $x=\Delta^{u}\pi_1\pi_2\ldots\pi_l$;

Step 1c. selecting a braid b at random to belong to a set $B_n(5\ l)$

Step 1d. calculating $x'=b^{-1}xb$, $a=b$;

Step 1e. generating a bit at random, if 1, calculating $x'=decycling(x')$, $a=a\pi_l$; if not 1, calculating $x'=cycling(x')$, $a=a\tau^{u}(\pi_l)$;

Step 1f. judging whether x' belongs to $SSS(x)$ and whether $l(x')\leq d$, if all the conditions are yes, outputting the braid pair(x, x') as the public key, a as the private key; if either of them is not, performing step 1e.

Claim 3 (Original) The digital signature scheme based on braid group conjugacy problem according to claim 1, wherein the process for obtaining $y=h(M)\in B_n(l)$ by using the hash function h in said step 2 comprises the following steps of:

Step 2a, selecting an ordinary hash function H, with a length of output $H(M)$ is l $[log(2,n!)]$, then dividing $H(M)$ into l sections $R_1||R_2||\ldots||R_l$ in equal at one time;

Step 2b, corresponding Ri to a permutation braid Ai, then calculating $h(M)=A1*A2\ldots Al$, that is the $h(M)$ required.

Claim 4 (Currently Amended) The digital signature scheme based on braid group conjugacy problem according to claim 1, ~~2 or 3,~~ wherein a integer *n* for the number of generators in a braid group is in the range of 20~30, an upper value of the braid length is $l=3$, $d=4$, and an left subgroup $n\text{-}m=4$.

Claim 5 (Original) A verifying method based on braid group conjugacy digital signature scheme, comprising the following steps of:

Step 1. a signature verifying party(V) obtaining a public key of a signatory (S) after receiving a message(M) and its signature *Sign(M)* transmitted from the signatory(S);

Step 2. calculating the message M by employing a system parameter hash function h, and obtaining $y=h(M)$;

Step 3. judging whether *sign(M)* and y are conjugate or not, if not, *sign(M)* is an illegal signature, and the verification fails; if yes, perform step 4; and

Step 4. calculating *sign(M)* x' and xy by using the public key of obtained S, and judging whether they are conjugate or not, if not, *sign(M)* is an illegal signature, the verification fails; if yes, *sign(M)* is the legal signature of message (M).

Claim 6 (Original) The verifying method based on braid group conjugacy digital signature scheme according to claim 5, wherein the form of obtaining the public key of signatory(S) in step 1 is an out-band form or a form of receiving the public key transmitted from signatory (S).

Claim 7 (Original) The verifying method based on braid group conjugacy digital signature scheme according to claim 5, wherein algorithm *BCDA* is employed in judging whether *sign(M)* and y are conjugate or not in step 3 and judging whether *sign(M)* x' and xy are conjugate or not in step 4.

Claim 8 (Original) A digital signature scheme based on braid groups conjugacy problem and verifying method thereof, parameters involved in this method comprising a signatory S, a signature verifying party V, a message M needing signature, an integer n for the number of generators in the braid group, an integer m for the number of generators in the left subgroup, an integer l for the upper bound of the length of a braid, a braid group $B_n(l)$, a left subgroup $LB_m(l)$, a right subgroup $RB_{n-1-m}(l)$, a one way hash function h mapped from bit sequence $\{0,1\}^*$ to braid groups $B_n(l)$; comprising the following steps of:

Step 1. the signatory(S) selecting three braids $x \in LB_m(l)$, $x' \in B_n(l)$, $a \in B_n(l)$, and making them meet $x'=a^{-1}xa$, moreover, with the known x and x', it is impossible to find a in calculation, and considering a braid pair(x',x) as a public key of the signatory *(S)*, a braid a as a private key of signatory *(S)*;

Step 2. signatory (S) using a hash function h for message (M) needing signature to get $y=h(M) \in B_n(l)$;

Step 3. generating a braid $b \in RB_{n-1-m}(l)$ at random, then signing the message (M) with the private key a and the braid b generated randomly to obtain $Sign(M)=a^{-1}byb^{-1}a$;

Step 4. the signatory (S) outputting the message (M) and its signature *Sign(M)* to the signature verifying party (V);

Step 5. the signature verifying party(V) obtaining the public key of signatory (S) after receiving the message(M) and the signature of message (M) *Sign(M)* transmitted from signatory(S);

Step 6. calculating message M by employing a system parameter hash function h, to obtain $y=h(M)$;

Step 7. judging whether *sign(M)* and y are conjugate or not, if not, *sign(M)* is an illegal signature, the verification fails; if yes, perform step 8; and

Step 8. calculating *sign(M)* x' and xy by using the obtained public key of signatory (S), and judging whether they are conjugate or not, if not, *sign(M)* is an illegal signature, and the verification fails; if yes, *sign(M)* is a legal signature of message (M).

Claim 9 (Original) The digital signature scheme based on braid group conjugacy problem and verifying method thereof according to claim 8, wherein generating the public key braid pair (x',x) and private key braid a of signatory (S) in said step 1 comprises the following steps of:

Step 1a. selecting a distance d between system parameter braid groups public key pair;

Step 1b. representing x into left canonial form $x=\Delta^{u}\pi_1\pi_2\ldots\pi_l$;

Step 1c. selecting a braid b at random to belong to set $B_n(5\ l)$

Step 1d. calculating $x'=b^{-1}xb$, $a=b$;

Step 1e. generating a bit at random, if 1, calculating $x'=decycling(x')$, $a= a\pi_l$; if not 1, calculating $x'=cycling(x')$, $a= a\tau^u(\pi_l)$; and

Step 1f. judging whether x' belongs to $SSS(x)$ and whether $l(x') \leq d$, if all conditions are yes, outputting braid pair(x, x') as the public key, a as the private key; if either of them is not, performing step 1e.

Claim 10 (Original) The digital signature scheme based on braid group conjugacy problem and verifying method thereof according to claim 8, wherein the process for obtaining $y=h(M) \in B_n(l)$ by using hash function h in said step 2 comprises the following steps of:

Step 2a. selecting an ordinary hash function H, with a length of its output $H(M)$ is l $[log(2,n!)]$, then dividing $H(M)$ into l sections $R_1||R_2|| \ldots ||R_l$ in equal at one time; and

Step 2b. corresponding Ri to a permutation braid Ai, then calculating $h(M) =A1*A2...Al$, that is the $h(M)$ required.

Claim 11 (Currently Amended) The digital signature scheme based on braid group conjugacy problem and verifying method thereof according to claim 8, ~~9 or 10~~ wherein n for the number of the generation braids in the braid group is in the range of 20~30, an upper value of the braid length is $l=3$, $d=4$, and an left subgroup n-m=4.

Claim 12 (Original) The digital signature scheme based on braid group conjugacy problem and a verifying method thereof according to claim 8, wherein algorithm $BCDA$ is employed in judging

whether *sign(M)* and *y* are conjugate or not in step 7 and judging whether *sign(M) x'* and *xy* are conjugate or not in step 8.

Claim 13 (New) The digital signature scheme based on braid group conjugacy problem according to claim 2, wherein a integer *n* for the number of generators in a braid group is in the range of 20~30, an upper value of the braid length is $l=3$, $d=4$, and an left subgroup n-m=4.

Claim 14 (New) The digital signature scheme based on braid group conjugacy problem according to claim 3, wherein a integer *n* for the number of generators in a braid group is in the range of 20~30, an upper value of the braid length is $l=3$, $d=4$, and an left subgroup n-m=4.

Claim 15 (New) The digital signature scheme based on braid group conjugacy problem and verifying method thereof according to claim 9, wherein *n* for the number of the generation braids in the braid group is in the range of 20~30, an upper value of the braid length is $l=3$, $d=4$, and an left subgroup n-m=4.

Claim 16 (New) The digital signature scheme based on braid group conjugacy problem and verifying method thereof according to claim 10, wherein *n* for the number of the generation braids in the braid group is in the range of 20~30, an upper value of the braid length is $l=3$, $d=4$, and an left subgroup n-m=4.